Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1123 Gr. 01
Titre : Sécurité de l'infonuagique et des services web
Session : Automne 2026 **Horaire et local**
Professeur : Caissy, David

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera familier.e avec les enjeux de la sécurité dans l'infonuagique et les services web, et sera capable de mettre en œuvre des solutions pour sécuriser les infrastructures infonuagiques et les services Web.

Contenu

Modèles de service (SAAS, PAAS, IAAS) et de déploiements (public, privé, communautaire, hybride) de l'infonuagique. Techniques et outils de virtualisation. Architecture d'une application Web. Éléments de base du langage SQL. Vulnérabilités, attaques et menaces dans le nuage et les services web (brute force, escalade de privilèges, XSS, injection de code, DDoS, etc.). Recommandations de l'OWASP (Open Web Application Security Project). Techniques de protection des données, des infrastructures et des applications dans le nuage (pare-feu, tests, etc.). Méthodologie d'évaluation de la sécurité applicative. Gestion des risques dans le nuage et aspects légaux de la sécurité dans le nuage et les applications Web. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

L'objectif de cette activité est que l'étudiante ou l'étudiant soit en mesure d'identifier les menaces et vulnérabilités de l'infonuagique, évaluer les méthodes d'attaque et gérer les risques de manière proactive. Il saura également sécuriser les applications infonuagiques et mettre en place la surveillance et l'automatisation de la sécurité, assurant ainsi une sécurité robuste et une conformité continue.

3. Stratégies pédagogiques :

Il s'agit d'un cours magistral en mode **non-présentiel avec deux examens en présentiel**. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Des travaux pratiques seront également réalisés afin de consolider les concepts présentés durant les séances de cours.

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont :

- **Microsoft Teams**. Un guide d'utilisation de Microsoft Teams est disponible sur le site de l'UQO : https://uqo.ca/guide-utilisateurs/formation-video-microsoft-teams
- Une connexion Internet, une webcam et un microphone.
- La suite **Office 365** (les étudiant(e)s ont un accès gratuit à la suite Office 365 : https://uqo.ca/sti/outils-numeriques).

4. Heures de disponibilité ou modalités pour rendez-vous :

Période de consultation sur rendez-vous seulement par courriel : david.caissy@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates

1	**Chapitre 1 : Introduction** • Modèles de service (IaaS, PaaS, SaaS) • Modèle de responsabilité partagée • Modèles de déploiements • Confidentialité, intégrité et disponibilité	8 sep. 2026
2	**Chapitre 2 : Gestion de l'identité et des accès** • Identification, authentification et autorisation • Niveaux d'assurance • Identités internes, externes et hybrides • Identités humaines et applicatives • Facteurs d'authentification et authentification multifacteur (MFA) • Modèles de contrôle d'accès	15 sep. 2026

3	**Chapitre 3 : Authentification unique**
	• Authentification unique (SSO)
	  ○ OAuth 2.0
	  ○ OpenID Connect
	  ○ SAML 2.0
	• Fournisseurs d'identité
	• Groupes et rôles de sécurité
	• Gestion des accès privilégiés (PIM)
	
	Travail Pratique 1 : Création d'une application Web dans Microsoft Azure (25 sep. 2026)
		22 sep. 2026

4	**Chapitre 4 : Accès conditionnels et protection du périmètre** • Politiques, stratégies et modèles d'accès conditionnels • Principales composantes de protection du périmètre **Travail Pratique 2 :** Configuration de l'authentification unique de Google pour une application Web dans Microsoft Azure (2 oct. 2026)	29 sep. 2026
5	**Chapitre 5 : Gestion des secrets** • Chiffrement des données au repos • Gestion des secrets • Système de gestion des secrets • Modèles de gestion des clés de chiffrement	6 oct. 2026
6	**Semaine d'études**	13 oct. 2026
7	**Chapitre 6 : Infrastructure à clés publiques** • Notions de cryptographie • Chiffrement des communications • Certificats de sécurité **Travail Pratique 3 :** Création d'une autorité de certification de base (Root CA) et signature d'un certificat de sécurité (23 oct. 2026)	20 oct. 2026
8	**Examen de mi-session (en présentiel)**	27 oct. 2026

9	**Chapitre 7 : Pare-feu et gestion des API** • Types de pare-feu • Réseaux virtuels et sous-réseaux • Groupe de sécurité réseau • Gestion des API • Service-à-Service (S2S)	3 nov. 2026
10	**Chapitre 8 : Architecture sécurisée** • Segmentation des réseaux et des environnements • Défense en profondeur • Architecture à confiance zéro • Protection contre le déni de service • Accès privé **Travail Pratique 4 :** Création d'une machine virtuelle dans Microsoft Azure (13 nov. 2026)	10 nov. 2026
11	**Chapitre 9 : Automatisation de la sécurité** • Gouvernance et conformité • Infrastructure en tant que code (IaC) • Gouvernance en tant que code (GaC) • Conformité en tant que code (CaC)	17 nov. 2026
12	**Chapitre 10 : Détection d'incidents de sécurité** • Journaux de sécurité • Détection et gestion des alertes de sécurité • Planification de la reprise après sinistre **Travail Pratique 5 :** Configuration d'un groupe de sécurité réseau (NSG) (27 nov. 2026)	24 nov. 2026
13	**Chapitre 11 : Centre d'opérations de sécurité et Dark Web** • Systèmes de gestion des informations et des événements liés à la sécurité • Gestion des incidents de sécurité • Réseau Tor, Deep Web et Dark Web • Recommendations de l'Open Web Application Security Project (OWASP) • Normes de vérification de la sécurité des applications (ASVS)	1 déc. 2026

14	**Chapitre 12 : DevSecOps**
	• Gestion de la configuration
	• DevOps et DevSecOps
	• Audit en cybersécurité et conformité
	  ○ Protection de la vie privée
	  ○ Conformité aux normes de l'industrie
	  ○ Évaluation de sécurité et autorisation
		8 déc. 2026

15	**Examen final (en présentiel)**	15 déc. 2026

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs du cours. Dans le cas spécifique du cours **Sécurité de l'infonuagique et des services web**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session (en présentiel) :** 30 %
- **Examen final (en présentiel) :** 40 %

- **5 travaux pratiques (6% chacun) :** 30 %

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.

Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.

Ensemble, participons à une culture de respect.

Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au biph@uqo.ca

8. Principales références :

- Notes de cours disponibles sur Moodle
- **Sécurité dans le Cloud AWS** (https://aws.amazon.com/fr/security)
- **Documentation sur la sécurité Azure** (https://learn.microsoft.com/fr-ca/azure/security)
- **Mesures de protection du nuage du gouvernement du Canada** (www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32787)

9. Page Web du cours :

https://moodle.uqo.ca/course/view.php?id=49881